**Android Malware Detection Analysis**

# **1. Executive Summary:**

Developed a System using deep learning algorithm to rectify and predicted whether an android system is malicious or clean. The dataset on which the model is trained consist of 328 attributes and 4465 records.

**2. Problem Statement:**

**Background:** Developing an Android malware detection system capable of accurately identifying novel and polymorphic malware strains in real-time, considering the rapidly evolving landscape of Android malware threats.

**Objective:** To Detect whether the Android system consist of Malware or not

**Scope:**

**Protecting Against Data Theft:** Protecting User Privacy & Preventing Financial Losses: Stealing sensitive information such as personal data, financial credentials, including contacts, messages, photos, and other files and location data. Malicious software often targets financial transactions and banking apps on Android devices. Detecting malware helps prevent unauthorized access to banking credentials and financial transactions, reducing the risk of financial losses for users.

**Avoiding Control over the Device:** If control over a device is taken, other malicious software can be installed which may worsen the situation.

**Ensuring System Integrity:** Malware can modify system settings, install unwanted applications, or tamper with system files, leading to instability, performance issues.

**Preventing Malicious Activities**: launching distributed denial-of-service (DDoS) attacks, sending spam emails, or spreading malware to other devices.

**Safeguarding Corporate Resources:** Many users use Android devices for work-related activities, accessing corporate email, documents, and networks. Malware on these devices can lead to data breaches, intellectual property theft, or unauthorized access to corporate resources.

# **3. Data Sources:**

Data Sources: Kaggle Platform

# **4. Methodology:**

Data Collection: Retrieve data from the Kaggle platform.

Data Preparation: Clean and prepare data in MySQL, Using Exploratory data analysis and Data preprocessing techniques handled missing values, and standardizing formats.

Analysis Techniques: Neural Network

Tools: Python (using libraries like pandas and scikit-learn) for modeling.

# **5. Expected Outcomes:**

Model that predicts Malware in Android system

Preventing Data privacy

Safeguarding system integrity

# **6. Risks and Challenges:**

Faced problem of having Less data - SMOTE

Handled too many insignificant variables

Managed Missing values & Duplicates values

# **7. Conclusion:**

In conclusion, detecting malware on Android devices is vital for keeping personal information safe, preventing financial harm, and maintaining the smooth operation of the system. By identifying and stopping malicious software, we protect against data theft, device takeover, and participation in harmful activities. Effective detection methods help build trust in the Android platform, ensuring a safer experience for users, developers, and businesses alike.